BILLING CODE: 3510-BX

DEPARTMENT OF COMMERCE

[Docket No. 150324295-5963-03]

Privacy Act System of Records, New System of Records

AGENCY: U.S. Department of Commerce, Office of the Secretary.

ACTION: Notice of new Privacy Act System of Records: "COMMERCE/DEPT-25, Access Control and Identity Management System."

SUMMARY: The Department of Commerce (Department) publishes this notice to announce the effective date of a Privacy Act System of Records notice entitled: COMMERCE/DEPT-25, Access Control and Identity Management System.

DATES: The system of records becomes effective on [Insert date of publication.]

ADDRESSES: For a copy of the system of records please mail requests to: Michael J. Toland, Departmental Freedom of Information and Privacy Act Officer, Office of Privacy and Open Government, 1401 Constitution Ave, NW, Room 52010, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Michael J. Toland, Department Freedom of Information and Privacy Act Officer, Office of Privacy and Open Government, 1401 Constitution Ave, NW, Room 52010, Washington, DC 20230.

SUPPLEMENTAL INFORMATION: On May 8, 2015, and June 29, 2015, the Department published and requested comments on a proposed new Privacy Act System of Records notice entitled: COMMERCE/DEPT-25, Access Control and Identity Management System. The system serves to provide electronic physical access control, intrusion detection and video management solutions to ensure the safety and security of DOC assets to include people, facilities, information and property. The system controls access to only those authorized as

well as aids in the monitoring, assessment and response to security and emergency related incidents. By this notice, the Department is adopting the proposed new system as final effective [Insert date of publication].

Public Comments and Responses

Interested parties were afforded the opportunity to participate in the rulemaking process through the submission of written comments on the proposed new systems of records notice (SORN). The Department received five public submissions in response to the proposed SORN. Due consideration was given to each comment received and the Department's responses to those comments are noted below.

One commenter recommended adding language under the Safeguards section to "address how the records/system is planned to address insider threats." The Department disagrees with this commenter's suggestion. The addition of such language would potentially impact the effectiveness of the Department's Insider Threat Program.

Several commenters urged the Department to withdraw this proposed system of records and to "refrain from implementing any intrusive system that needlessly monitors the movements of its employees." In support of their suggestion, two commenters said that "The Department has not explained the need for tracking employees' every physical movement when on-site, which, in the proposed system of records, would go so far as to include monitoring the buttons employees strike on their work station keyboards." Further, those commenters raised concerns about employee morale and the security of the system. In addition, several commenters submitted the view that this SORN does not adequately describe provisions or processes to insure the safety and integrity of employees' sensitive personally identifiable information.

The Department disagrees with these comments. The system of records covered by this SORN are subject to the Federal Information Security Management Act (FISMA), which requires that controls be put in place to protect IT systems and the information contained within. Additionally, Privacy Impact Assessments have been conducted on these systems to further define procedures for protecting personally identifiable information (PII) and address the impact on employees' privacy. Further, the SAFEGUARDS section of this notice describes methods for protecting information maintained in this system. For example, this section mentions that "electronic records are password-protected or PKI-protected, consistent with the requirements of [FISMA] (Pub. L. 107-296), and associated OMB policies, standards and guidance from the National Institutes of Standards and Technology, and the General Services Administration, all records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards." It should be noted that safeguards should be described in general terms and to the extent they would not compromise system security, which serves as an added layer of protection for employees' data.

One commenter suggested that it was unclear whether the Department is attempting to either 1) create a new database with all the information set forth in the SORN, or 2) come into compliance with statutes and regulations concerning employee data that the Department already has in an existing system. The Department is issuing this new SORN to ensure that the Department is in compliance with the Privacy Act, as amended, 5 U.S.C. § 552a(e)(4) and (11); and OMB Circular A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals for all categories of information covered by DEPT-25. This SORN covers some similar categories of information as a government-wide SORN, GOVT-7, "Personal Identity Verification Identity Management System (PIV IDMS)." After a review,

the Department decided to implement a more specific SORN with respect to this system of records.

The same commenter further suggested that if the SORN is bringing the Department into compliance, then certain personnel actions involving employee data collected prior to publication of the SORN are called into question. This comment goes beyond the scope of the content and adequacy of this SORN.

Another commenter proposed that implementation of the SORN will result in a significant staffing increase to administer and monitor the program. The Department disagrees. Adequate resources are available within the Department's Office of Security and Office of the Chief Information Officer to administer and monitor the program as it relates to Access Control and Identity Management.

One commenter suggested that employees will have difficulty determining what information the Department is maintaining on them and how to obtain the information kept. The Department disagrees with the commenter's suggestion. This notice has a section, CATEGORIES OF RECORDS IN THE SYSTEM, which enumerates the information collected from individuals. Should an employee need additional clarification on information collected and maintained on him or her in this system of records, the employee can file a Privacy Act request following the procedures outlined in the NOTIFICATION PROCEDURE section of this notice. With regard to obtaining information kept, another section, RECORDS ACCESS PROCEDURES, provides instructions on how an individual can request access to records on himself or herself. It should be noted that under the SYSTEM EXEMPTIONS FROM CERTAIN PROVISION OF THE ACT section, all information and material in the record which meets the criteria of the subsections listed under parts of General Exemptions

and Specific Exceptions of the Privacy Act are exempted from the notice, access, and contest requirement. Employees should refer to the aforementioned SYSTEM EXEMPTIONS FROM CERTAIN PROVISION OF THE ACT section of this notice for additional information about the requirements for exemptions.

Another commenter asked whether an employee will be monitored more closely based on political or religious or other beliefs. There is no authority for an agency to monitor its employees based on their political or religious beliefs. In fact, Section 552a(e)(7) of the Privacy Act, prohibits an agency from maintaining a record of how an individual exercises rights guaranteed under the First Amendment, and there are a number of other statutory and policy protections in place that guard against this type of behavior. Therefore, this commenter's concern is misplaced.

Other commenters expressed concerns about how the Department would employ the use of key-stroke monitoring. In particular, they wanted to know whether the information would be used for all agency employees, even those not suspected of committing any violations of Federal law or Department policies. One of the commenters stressed that "It is a well-accepted IT Security policy within the Federal workspace (and also the private sector) that key-logging programs are insidious, and are used by cyber-criminals to mine data surreptitiously in order to gain unauthorized access to protected information resources. Their presence in the workplace is forbidden for these reasons." The Department would like to clarify for these commenters that key-stroke monitoring, which is included in this system of records, would be used under appropriate conditions to evaluate anomalous behavior, including suspected or established violations of Federal law or Department policies.

One commenter asked if the phrase "agency, entity or persons" referred to in a routine

use includes data sharing with private sector companies or "entities." The Department notes that two routine uses, numbers 12 and 13, found at 80 FR 26356 (May 8, 2015), of the notice contain the phrase "agency, entity or persons." Routine use number 12 deals with sharing information when a breach occurs, while routine use 13 concerns sharing information "for the purpose of performing audit or oversight operations as authorized by law." In both cases, sharing of information may occur with private sector companies or "entities" that have been contracted to provide the support or services described in the aforementioned routine uses. Information shared is kept to the minimum necessary to accomplish the prescribed tasks. It should be noted that pursuant to Federal Acquisition Regulations (FAR) Part 24, Privacy Act clauses are required to be included with any contracts for which a contractor is required to be involved with the design, development, or operation of a system of records on individuals to accomplish an agency function. Under one such clause, FAR 24.104, the contractor agrees to "comply with the Privacy Act of 1974 (Act) and the agency rules" when using any system of records on individuals in the performance of duties specified in the work statement. The notice also contains a routine use, number 9, which allows records from this system to "be disclosed to a contractor of the Department having need for the information in the performance of the contract, but not operating a system of records with the meaning of 5 U.S.C. 552a(m)."

The same commenter stated, "Further, according to this new system, Commerce could disclose information to Agencies, entities and persons, to prevent, minimize, or remedy 'a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of the system.'" This commenter went on to ask whether some interested party in a civil lawsuit could request and gain access to data from this system of records under any of

the notice's routine uses. The commenter is referring to routine use number 12, which concerns providing information for breach mitigation and notification. Provision of data from this system of records to an interested party engaged in a civil lawsuit is not part of this routine use.

One commenter suggested that according to the routine use 2 listed in the *Federal Register*, 80 FR 26536 (May 8, 2015), "protecting the interest of the Department is an accepted justification for referring relevant records, 'as a routine use, to the appropriate agency, whether [F]ederal, state, local, or foreign, charged with the responsibility of…protecting the interest of the Department.' This seems to give the Department a lot of leeway to protect itself from having to disclose possible breaches, errors, or even somewhat embarrassing information. It also seems to give leeway to selectively identify which employees might be disciplined for wrongdoing or infractions that hurt the Department." The Department disagrees with this commenter's assertion. The Department has a duty to appropriately safeguard personally identifiable information (PII) in its possession and to prevent its compromise in order to maintain the public's trust. Additionally, the Department, like each Federal agency covered under OMB Memorandum M-07-16, "Safeguarding Against and responding to the Breach of Personally Identifiable Information," is required to develop a breach notification policy and plan, and to establish a core management team responsible for responding to the breach of PII. To fulfill its commitment to employees, as well as to satisfy OMB requirements, the Department has developed and fully expects all staff to follow a Personally Identifiable Information (PII) and Business Identifiable Information, and Privacy Act (PA) Breach Notification Plan. There are no exceptions to following the plan, as well as reporting breaches. The Department has also established a Computer Incident Response

Team (CIRT) and the Department of Commerce PII Breach Response Task Force for reporting and managing breaches.

One commenter asked how the Department would "ensure that the usage of the new system of records will be limited in its scope[.]" For instance, the individual proposed that the new system poses a risk of the data being used for purposes not intended in this notice. This commenter also suggested that "the collection of badge in/badge out data, time in/time out data, login/logout data, keystroke monitoring and logs of internet activity all point to using this dataset to monitor, by hours and minutes, employees' schedules and work patterns. These paradata are not reliable indicators of the time employee's work and they should not be used for disciplinary purposes." Employees are responsible for performing their duties at acceptable levels and for conducting themselves in a manner consistent with law, regulations, and policies. If an employee would be found to have behaved in a way that violated these standards, the Department will use evidence to prove those failings by the appropriate statutory standard. Most acts of misconduct are proved by evidence other than the data at issue here, but this data may constitute evidence of misconduct under certain circumstances. The Department's usage of badge records will be undertaken in accordance with this SORN, and there are policies in place that ensure evidence of employee misconduct used in disciplinary actions is truthful, reliable, and probative of the misconduct that is charged.

One commenter proposed that "to ensure security of this system and to protect employees, there should be a system of records of who accesses [the] information [maintained in this system of records], when, for what purposes, and how that information was authorized." The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, defines conditions under which agencies may disclose information from records retrieved by a person's name or other

personal identifier. As a general rule, the Department may not disclose a record about such a person, except upon a written request by, or with the prior written consent of, that individual. However, it is important to note that to carry out its statutory responsibilities the Department at times may need to disclose information in Privacy Act records for purposes other than those listed in the Act. With this in mind, under certain specific conditions, the Privacy Act authorizes disclosure of information in a record, whether or not the person to whom the information relates has requested or consented to disclosure. For instance, the Act authorizes disclosures under, 5 U.S.C. § 552a(b), Conditions of Disclosure. The Act also authorizes agencies, such as the Department, to make such disclosures, once they publish a description of what are called the "routine uses" of information in their records.

A level of protection is afforded to individuals because the routine use must be published in the Federal Register, and the routine use must include categories of users and the purpose of the use. A routine use must also be compatible with the purpose for which the information was collected. Further, another level of protection may be evidenced through the fact that publication of routine uses by the Department does not *require* it to disclose information in a record - it merely *permits* the Department to disclose information when deemed appropriate or necessary by the Department. The Department's policy is to carefully decide whether a disclosure of information permitted by a routine use is appropriate or necessary, based on the totality of the circumstances. If the Department believes that disclosure of information protected by the Privacy Act is appropriate or necessary in a situation not covered by a routine use, or by any other exception to the act's general prohibition on disclosure, it will seek written consent for the disclosure from the person to whom the record pertains. Lastly, a level of protection comes from the Privacy Act

requirement for agencies to maintain an accurate accounting of certain disclosures, except in instances where disclosure is made to the subject of the record. This accounting must be maintained for a period of five years or the life of the record, whichever is longer, and must be made available upon request by the subject of the record, except for disclosures related to law enforcement activities. With regard to this accounting of disclosures, according to the OMB Privacy Act Implementation Guide, published in the *Federal Register* on July 9, 1975 (40 FR 28948-28978), "the intent was to view the accounting of disclosures as other than a system of records and to conclude that an accounting need not be maintained for the disclosures from the accounting of disclosures."

Several commenters expressed concerns that this system of records could create Privacy Act issues. Along those lines, one commenter specifically questioned the protections afforded employees when data is released under one or more of the exemptions identified in notice's the SYSTEM EXEMPTIONS FROM CERTAIN PROVISIONS OF THE ACT section. While system exemptions from certain provisions of the Privacy Act have been identified in this notice, those provisions are allowed by and used following the Privacy Act; they do not revise the Act. Further, it was recognized in the OMB Privacy Act Implementation Guide, published in the *Federal Register* on July 9, 1975 (40 FR 28973), that "'due process' in both civil action and criminal prosecution will assure that individuals have a reasonable opportunity to learn of the existence of, and to challenge, investigatory records, which are to be used in legal proceedings. To the extent that such an investigatory record is used as a basis for denying an individual any right, privilege, or benefit (including employment) to which the individual would be entitled in the absence of that record, the individual must be granted access to that record except to the extent that access would reveal the identity of a confidential

source."

Two other commenters stated that the notice does not provide any provisions or processes regarding any final disposition of employee personal information (PII) once it has been disclosed to other agencies, entities, or persons. This comment goes beyond the requirements of the Privacy Act.

More than one commenter submitted the view that the routine uses listed in this notice may result in matching programs as described in 5 U.S.C. § 552a(a)(8). Further, commenters added that if the Department engages in any matching program, it must follow matching program requirements outlined in 5 U.S.C. § 552a(o). The Department recognizes the concerns commenters may have about matching programs with respect to this system of records and would like to assure those commenters that should the Department engage in matching programs as defined by the Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503 ("Computer Matching Act"), it will follow applicable procedural requirements. The Computer Matching Act, which amended the Privacy Act, establishes procedural safeguards affecting agencies' use of Privacy Act records when conducting certain types of computer matching programs. These procedures ensure the integrity, privacy, and verification of data used in computerized matching operations, and the Department intends to fully comply with these procedures should it engage in matching programs covered by the Computer Matching Act.

Multiple commenters requested that the Department work in collaboration with unions to create a more useful and less intrusive monitoring system of records. The Department has proposed to the Labor Management Forum Members, to hold a meeting(s) to discuss the appropriate process for access, reviewing and acting upon data collected through an electronic

process. Those meetings should begin in early FY 16. In the view of the same commenters, the Department should provide notice and allow bargaining under Federal Services-Labor Management Relations Statute, 5 U.S.C. §§ 7101-7135. The issuance of this notice by the Department is a matter of compliance with the Privacy Act and in no way interferes with labor's right to bargain over matters that relate to a change in working conditions.

In the view of one of the commenters, "the Department failed to make any attempt to notify its labor partners of these proposed changes." In order to address any concerns with notification, the Department extended the comment period for this SORN so that labor unions had ample time to submit comments.

One commenter wondered if the data expected to be obtained through COMMERCE/DEPT-25 was worth the enormous investment of time in labor-management negotiation, Congressional review, and potential negative response from Department employees over such a program. Through a variety of methods, the Department already collects employee data. This SORN ensure employees understand the system of records and the means through which they can ensure that their data is correct.

Several commenters conveyed their concerns about data security regarding this system of records, especially in light of the recent OPM data breaches in which millions of current and former Federal employees' records were compromised. One of those commenters put forth that while the notice listed safeguards for the system, "it was unclear whether the data would be encrypted." Another commenter raised concerns about identity theft and the potential use of data for unintended purposes that increases risks and reduce privacy protections, especially in the context of data aggregated in one database. The Department recognizes these concerns and is applying lessons learned from recent high-profile cyber

events. As with all Department IT systems, the appropriate FISMA controls, specifically those regarding encryption, will be applied based upon the security categorization of the system and the data contained within the system. The Department has taken the potential risk related to data aggregation into consideration with respect to this system of records. With this in mind, the Department has applied and will continue to apply all appropriate FISMA controls based upon the security categorization of a system.

More than one commenter suggested that the Department provided insufficient [business] justification for this system of records in the Purposes section. The Department disagrees with this suggestion. As articulated in the PURPOSES section, this notice is intended to ensure protection of Department assets.

One commenter suggested that the system of records should exclude home telephone numbers because "the connection of home telephone to the purposes stated in the notice is unexplained and unclear." While this notice is intended to let employees know what information "may" be collected and what possible use of that information exists, the collection of a "home" telephone number for this system of records is not a mandatory requirement and as such the individuals have the option of not providing their home telephone number. However, having contact information, such as home telephone number, serves a number of purposes, including but not limited to Continuity of Operations (COOP) activities, telework, and notification of family in the event of an emergency.

The same commenter also submitted that "social security numbers [(SSN] should be excluded and replaced by an employee number." The commenter said the "connection of [SSN] to the purposes stated in the notice is unexplained and unclear." The Department has not adopted this suggestion, because the use of SSNs in this system of records is essential due

to the various categories of individuals in the system. For instance, government contractors would not have an employee number. SSNs are also necessary for the Department to accurately report employees' earnings, so they get the proper credit towards their social security benefit. Even with the addition of an employee number, the Department would still need to capture the social security number for the reasons stated above.

The Department has considered this comment and to help clarify the meaning of cellular numbers, the term "government and personal" will be added before "cellular telephone number" under the CATEGORIES OF RECORDS IN THE SYSTEM section. It should be noted that the Department collects both personal and government cell numbers, because in many cases employees have dropped land line service, so their cell number is their personal home number. As previously stated, having contact information, such as a telephone number, serves a number of purposes, including but not limited to COOP activities, telework, and notification of family in the event of an emergency.

One commenter suggested that "if a security problem does exist within the Commerce Department and its various Agencies that requires [the] level of attention [identified in this system], consultation with authoritative IT Security professionals on implementing a best-practices solution would seem to be a simpler, more cost-effective, and less intrusive alternative." The Department appreciates this commenter's view, and it regularly consults with other Government agencies and industry regarding best-practices for the identification, mitigation, and response to cyber related issues and concerns with a view towards improving Departmental capabilities. The Department proactively places emphasis on all phases of the NIST Cyber Security Framework – Identify, Protect, Detect, Respond, and Recover.

More than one commenter maintained that the descriptors in this notice need to be

defined in more detail. For instance, some suggested that more information should be provided for the Purposes, Retrievability, and Record Sources sections. One of the commenters added that more clarity was needed for the RETRIEVABILITY section, specifically for the statement "Information may be retrieved…by automated search based on extant indices and automated capabilities…" While the Department disagrees with the commenters that the descriptors in this notice need to be defined in more detail within the notice, it does agree that it would be beneficial to create a document explaining SORN descriptors. As a way to provide explanations about the different sections of a SORN, the Department has produced a fact sheet about SORN descriptors, which will be made available on its public website under the Office of Privacy and Open Government webpage at http://www.osec.doc.gov/opog/.

One of the same commenters suggested that a plain language document should be provided that discusses this notice and its relationship to the Privacy Act. The Department agrees with the commenter that is would be beneficial to create a document explaining this notice and its relationship to the Privacy Act. As a start to providing the type of information requested, the Department has produced a fact sheet about SORN COMMERCE/DEPT-25, which will be made available on its public website under the Office of Privacy and Open Government webpage at http://www.osec.doc.gov/opog/.

In the view of another commenter, this notice did not provide an indication of "how long information is retained and how that duration relates to the proposed uses." The Department notes that every SORN, including this one, contains a RETENTION AND DISPOSAL section, which describes the policies and guidelines in place with regard to the retention and destruction of records in this system.

October 29, 2015_
Date

_____
Michael J. Toland
Department of Commerce
Freedom of Information and Privacy Act Officer

For the reasons stated in the preamble, the Department of Commerce amends the Privacy Act System of Records: "COMMERCE/DEPT-25, Access Control and Identity Management System," with the minor change as follows:

■ To help clarify the meaning of cellular numbers under the CATEGORIES OF RECORDS IN THE SYSTEM section, the term "government and personal" will be added before the language "cellular telephone number".

[FR Doc. 2015-28056 Filed: 11/3/2015 11:15 am; Publication Date: 11/5/2015]